COUNTY OF LOS ANGELES
CHIEF INFORMATION OFFICE
500 West Temple Street
493 Kenneth Hahn Hall of Administration
Los Angeles, CA 90012

JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

June 8, 2006

To: Department Heads

From: Jon W. Fullinwider
Chief Information Officer

Subject: **PROTECTING EMPLOYEE/SENSITIVE CLIENT DATA RESIDING ON LAPTOP OR OTHER TYPES OF PORTABLE COMPUTING DEVICES**

On June 7, 2008, I met with members of your IT staff to discuss potential solutions for protecting employee/client confidential data that may reside on mobile computing devices (i.e., laptop personal computers, personal data assistants (PDAs) and memory storage devices). There was overwhelming participation and absolute agreement that this was a problem that needed to be dealt with.

The scope of the problem was discussed in light of the recent incidents within the County and other government agencies and private sector companies. Clearly, the easiest solution would be to establish a Board policy prohibiting the placement of any employee or client confidential data on portable computing devices. However, for valid business reasons, that direction would not prevail and a more accommodating solution had to be identified. Using the criterion that whatever solution selected needed to be effective and easily enforceable, it was unanimously agreed that encryption (solution to be determined) would be implemented on all laptops and PDAs ensuring that all data stored on these devices would be encrypted automatically. While there are several solutions available to accomplish this objective, a Task Team (committee) was formed to assist in the identification and selection of a countywide standard. The Committee understands the importance of the objective and is prepared to move very quickly in identifying a solution.

In the mean time, a Board Policy is being developed that will articulate the need, criterion for use and actions to be taken in the event of future unauthorized disclosure of employee/client confidential data. Lastly, the policy will endorse the technology solution identified to encrypt all data on laptop or other types of PDAs.

I will keep you informed as to our progress and ensure that you have adequate time to review drafts of all policies and/or guidelines that will be developed prior to seeking Board approval. Recognizing the importance of this undertaking, we are targeting the end of July or early part of August to have a solution ready for Board approval.

JWF:ygd

c: Board of Supervisors
IT Deputies
IT Managers

P:\Final Documents\CIO\security\sensitive data protection_mtg results.doc